



February 28, 2013

VIA ECFS

Ms. Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, DC 20554

**Re: EB Docket No. 06-36; Annual Customer Proprietary Network Information
Compliance Certification**

Dear Ms. Dortch:

Pursuant to 47 C.F.R. §64.2009(e), Signal Point Corp. hereby submits its Annual Customer Proprietary Network Information Compliance Certification for 2012. Signal Point purchased substantially all the assets of RNK, Inc. (Filer ID 820199) pursuant to a bankruptcy sale. Signal Point is in the process of transferring RNK's regulated assets, and is managing RNK with respect to such assets during the transition. Therefore to the extent required, please accept this annual certification on behalf of RNK and Signal Point. Should you have any questions regarding this submission, please direct them to the undersigned at (781) 613-9148.

Sincerely,

Matthew Tennis
Senior Counsel
Manager of Regulatory Affairs

Cc: Best Copy and Printing, Inc. via email [FCC@BCPIWEB.COM]

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2012

Date filed: February 28, 2013

Name of company(s) covered by this certification: Signal Point Corp.*

Form 499 Filer ID: 829488

Name of signatory: Aaron Dobrinsky

Title of signatory: President

I, Aaron Dobrinsky, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules (See attachment A).

The company has not taken any actions (proceedings instituted or petitions filed by the company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may be subject to enforcement action.

Signed 

*Signal Point Corp. purchased substantially all the assets of RNK, Inc. (filer ID 820199) in September 2012 pursuant to a bankruptcy sale. RNK's licenses are currently being transferred to Signal Point. While the transfer is pending, Signal Point Corp. is managing RNK with respect to its regulated assets, including filing of this CPNI certification on its behalf with respect to regulated assets under RNK's control prior to the asset purchase.

Attachment A

Statement of Signal Point Corp. Compliance Procedures

1. **Signal Point's Use of CPNI:** Signal Point's operating procedures ensure that Signal Point is in compliance with the Commission's CPNI Rules. Except as required or permitted by law or Subpart U of Title 47 of the Code of Federal Regulations; 47 CFR 64.2001, et seq., Signal Point does not use CPNI.

Signal Point has internal policies and procedures in place to educate employees as to the confidential nature of CPNI and when disclosure of CPNI is appropriate. Signal Point's Employee Manual, which employees are required to review and abide by, includes express policies detailing Signal Point's use of CPNI and identifying its proprietary nature. Signal Point customer service personnel have also been instructed in the proper usage and protection of CPNI when dealing with customer service requests. Further, Signal Point's Master Service Agreement, available to the public on its company website, includes express provisions referencing Signal Point and its business partners' use of CPNI and identifying both the proprietary nature of CPNI and the necessity to safeguard such information. In addition, Signal Point does not use or otherwise disclose CPNI for marketing purposes. Finally, Signal Point releases CPNI pursuant to lawfully executed instruments or authorizations, and in limited circumstances as described in Section 2.

2. **Carrier Authentication Requirements:** Presently, Signal Point does not disclose CPNI over the phone when customers call Signal Point. Customers with online accounts can access CPNI through the use of a username/password combination. If a customer requests CPNI, and does not have an online account, procedures are in place to allow Signal Point employees to coordinate internally with legal and regulatory departments to carry out disclosure on a case-by-case basis in accordance with the CPNI Rules. For instance, Signal Point may provide CPNI to a requesting customer by sending it to their address of record. Signal Point may also provide routine customer service utilizing CPNI provided by a customer over the phone. Procedures such as these ensure that customers receive technical support and information related to their services with minimal risk of unauthorized disclosure of CPNI. Certain business customers are also provided CPNI information via invoices which are sent to the customer at their address of record.

Signal Point offers some of its business customers access to their CPNI using an online, automated system. This system is isolated from the public internet, in that only unique customer servers are recognized by Signal Point's system, based in part on the server's physical location. While Signal Point believes this method of disclosure is equivalent to, if not more secure than, password protection, in order to effect full technical compliance with the CPNI Rules, Signal Point has put into place notice and contractual procedures to ensure that each business customer

who acquires CPNI by this method is aware of the CPNI Rules and also agrees to safeguard CPNI in accordance therewith.

3. **Notice of Account Changes:** Signal Point customers are notified whenever changes occur in their accounts, such as password or address of record changes, generally via email notification.
4. **Notice of Unauthorized Disclosure:** Signal Point's operating procedures ensure that Signal Point is in compliance with the Commission's CPNI Rules regarding unauthorized disclosure of CPNI. In the event a Signal Point employee suspects an unauthorized disclosure of CPNI has occurred, Signal Point's internal procedures provide that the employee notify their supervisor, who coordinates with Signal Point's legal and regulatory departments to determine if a breach has occurred. In the event of breach, Signal Point's procedures provide that its legal and regulatory departments notify the United States Secret Service (USSS) and the FBI within seven business days through the online central reporting facility, and proceed according to the CPNI Rules.

Signal Point has put into place procedures to maintain records of unauthorized disclosures of CPNI, notifications to the USSS and the FBI regarding those disclosures, as well as the USSS and the FBI response to the notifications for a period of at least two years. These records will include the following, if available, for each unauthorized disclosure: the date Signal Point discovered the unauthorized disclosure, the date notice was sent to the USSS and FBI, a detailed description of the CPNI that was disclosed, and any other circumstances of the disclosure not covered under the above.

5. **Opt-in/Opt-out Procedures:** Presently, Signal Point does not utilize CPNI, for sales or marketing purposes, that would require the use of opt-in or opt-out procedures as described in the CPNI Rules.
6. **Signal Point Internal Policy and Disciplinary Policy:** Signal Point has adopted a policy requiring employees to comply with the CPNI Rules. Signal Point's policy provides that any employee who fails to comply with the Rules and Signal Point's internal policies is subject to severe disciplinary procedure, up to and including immediate termination depending on the nature of the offense and whether or not the noncompliance was intentional.